What is claimed:

1. A system for electronic transactions comprising:

an electronic card having,

a cryptographic service for encryption and decryption,

a data area for storing cardholder information, and

a data area for storing service provider information;

a service provider member terminal responsive to activation of the electronic card; and

a service provider terminal in communication with the service provider member terminal, the service provider terminal decrypting communication from the service provider member terminal and encrypting communication to the service provider member terminal, the service provider member terminal encrypting communication to the service provider terminal and decrypting communication from the service provider terminal.

2. The system of claim 1 wherein the electronic card is a physical card.

3. The system of claim 1 further comprising software having the electronic card.

4. The system of claim 1 wherein the electronic card further comprises a card operating system for loading and updating cardholder information, changing access conditions, and managing the service provider data area.

5. The system of claim 1 wherein the electronic card performs external communication read/write operations, and communication protocol handling.

6. The system of claim 1 wherein the electronic card further comprises software to manage the electronic card.

7. The system of claim 1 wherein the electronic card further comprises application software.

8. The system of claim 1 wherein the electronic card further comprises applets.

9. The system of claim 1 further comprising an external system wherein the service provider terminal communicates with the external system.

10. The system of claim 1 wherein the data area for storing service provider information includes at least one service provider record, each service provider record comprising:

a name field indicating the service provider;
at least one key value;
a key-type indication indicating the type of the key value; and
an account information field containing information unique to each service provider.

11. The system of claim 10 wherein the service provider record further comprises an instrument-type indication indicating the type of instrument a service provider supports.

12. The system of claim 10 wherein the service provider record further comprises an access condition, which a user must satisfy to gain access to the service provider information.

13. A method of conducting an electronic transaction using an electronic card comprising:

formatting a key exchange request message at a member;
sending the key exchange request message from the member to a service provider;
generating a session key at the service provider;
formatting a key exchange response message including the session key at the service provider;
sending the key exchange response message from the service provider to the member; and
using the session key to conduct a transaction.

14. A method of conducting an electronic transaction using an electronic card comprising:

formatting a key exchange request message at a member, the key exchange request message has a member challenge for the service provider;

sending the key exchange request message from the member to a service provider;

generating a session key at the service provider;

formatting a key exchange response message including the session key at the service provider, the key exchange response message has a response for the member challenge and a service provider challenge for the member and sending it to the member;

formatting by the member a response for the service provider challenge and sending it to the service provider; and

using the session key to conduct a transaction. a

15. The method of claim 13 or 14 wherein the step of using the session key to conduct a transaction comprises the steps of:

formatting by a member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

16. The method of claim 15 wherein the member encrypts, using the session key assigned to him by the service provider, his account information, the transaction amount and sensitive transaction data in his transaction request message, the sensitive transaction data being information that is accessible only to the service provider.

17. The method of claim 15 wherein the member includes plain text in his transaction request message.

18. The method of claim 15 wherein the member includes the transaction identification assigned to him by the service provider, in his transaction request message.

19. The method of claim 15 wherein the member includes a response to a service provider challenge in his transaction request message.

20. The method of claim 15 wherein the service provider encrypts the response data for the member using member's session key and include the cryptogram as part of its transaction response message to the member.

21. The method of claim 15 wherein the service provider includes plain text in its transaction response message to the member.

22. The method of claim 15 wherein the service provider includes member's transaction identification in his transaction response message to the member.

23 The method of claim 15 further comprises the steps of:
formatting at the member, using the session key, a transaction acknowledgment message, including a digital signature of the sending member, and sending the transaction acknowledgment message to the service provider.

24. The method of claim 15 wherein the member encrypts, using the session key assigned to him by the service provider, his acknowledgment data in his acknowledgment message.

25. The method of claim 15 wherein the member includes plain text in his acknowledgment message.

26. The method of claim 15 wherein the member includes the transaction

identification assigned to him by the service provider, in his acknowledgment message.

27. The method of claim 15 wherein the member chooses to encrypt sensitive information in the transaction acknowledgment message, the sensitive information being information that is accessible only to the service provider.

28. The method of claim 13 or 14 of conducting a key exchange comprising:

generating a member challenge by the member;

encrypting by the member the member challenge using the service provider's public key and generating a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and member's public key;

singing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message to the service provider;

generating by the service provider a service provider challenge;

generating by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key and generating a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and the response to member challenge;

signing digitally by the service provider the key exchange response message;

sending digitally signed key exchange response message to the member;

encrypting by the member the member response for the service provider challenge using the session key and generating a third cryptogram;

attaching the third cryptogram to the next message going from the member to the service provider;

signing digitally by the member the next message going from the member to the service provider; and

sending the next message going from the member to the service provider to the service provider.

~~29. The method of claim 28 wherein the member uses different pairs of private and public keys for different transactions in the messages to communicate with the service provider.~~

~~30. The method of claim 28 wherein the key exchange request message and key exchange response message contain plaintext~~

~~31. The method of claim 28 wherein the member chooses to encrypt his own public key using the service provider's public key in the key exchange request message.~~

~~32. The method of claim 28 wherein the member and service provider chooses to encrypt sensitive information in the key exchange request message and the key exchange response message, the sensitive information being information that is accessible only to the service provider and the corresponding member.~~

~~33. The method of claim 28 wherein the service provider encrypts the response to the member challenge as part of the second cryptogram.~~

~~34. The method of claim 28 wherein the service provider encrypts transaction identification as part of the second cryptogram.~~

~~35. The method of claim 28 wherein the service provider includes a transaction identification as part of the plain text in the key exchange response message.~~

~~36. The method of claim 34 wherein the member uses the transaction identification in the next message going from the member to the service provider.~~

~~37. The method of claim 35 wherein the member uses the transaction identification in the next message going from the member to the service provider.~~

38. The method of claim 13 or 14 of conducting a key exchange between two members and a service provider comprises the steps of:

sending a key exchange request message from the first member to a second member;

combining at the second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

formatting a key exchange response message at the service provider including the session key for the first member, signing the response message, formatting a key exchange response message including the session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

39. A method of claim 13 or 14 wherein the step of conducting a transaction between two members and a service provider comprising:

formatting by a first member, using the first member's session key, a transaction request message, the transaction request message including a digital signature of the first member, and sending the transaction request message to a second member; and

formatting by the second member, using the second member's session key, a transaction request message;

combining by the second member, the second member transaction request message with the first member transaction request message, the combined transaction request message including a digital signature of the second member, and sending the combined transaction request message to a service provider;

formatting by the service provider, using the first member's session key, a transaction response message for the first member, including a digital signature of the service provider;

formatting by the service provider, using the second member's session key, a transaction response message for the second member;

combining the transaction response message for the first member with the transaction response message for the second member and forming a combined transaction response message, the combined transaction response message including a digital signature of the service provider;

sending the combined transaction response message to the second member;

separating at the second member, the transaction response message for the first member from the transaction response message for the second member;

forwarding by the second member the transaction response message for the first member to the first member.

40. The method of claim 39 further comprises the steps of:

formatting at a first member, using the first member's session key, an acknowledgment message, the acknowledgment message including a digital signature of the first member, and sending the acknowledgment message to a second member~~; and~~

formatting at the second member, using ~~the~~ second member's session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message and forming a combined acknowledgment message, the combined acknowledgment message including a digital signature of the second member, and sending the combined acknowledgment message to the service provider.

41. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in series comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a second member where the second member is a message router or participating member;

sending a key exchange request message from the second member to a next member, if the second member is a message router;

combining the second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange message to the next member if the second member is a participating member;

sending the combined key exchange request message to the next member if the current member is a message router;

combining a current member's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to a next member, if the current member is a participating member;

sending the combined key exchange request to a service provider if the current member is the last participating member or message router;

generating at the service provider different session keys for different participating members;

formatting, by the service provider, into one message, a key exchange response message including the different session keys for different participating members and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating member, the key exchange response message for itself from the key exchange response messages for the other participating members, and forwarding the remaining key exchange response messages to the other participating members in reverse order of the path for sending the combined key exchange request to the service provider, until the first member receives its key exchange response message.

42. The method of claim 13 or 14 of conducting a transaction using session keys between multiple members and a service provider arranged in series comprising the steps of:

formatting a transaction request message at a first member;

sending a transaction request message from the first member to a second member where the second member is a message router or participating member;

sending the transaction request message from the second member to a next member, if the second member is a message router;

combining the second member's transaction request message with the first member's transaction request message and sending the combined transaction message to the next member if the second member is a participating member;

sending the combined transaction request message to the next member if the current member is a message router;

combining a current member's transaction request message with a previous member's transaction request message and sending the combined transaction request message to a next member, if the current member is a participating member;

sending the combined transaction request to a service provider if the current member is the last participating member or message router;

formatting, by the service provider, into one message, a transaction response message and sending the combined transaction response message in reverse order of the path for sending the combined transaction request to the service provider; and

separating, by every participating member, the transaction response for itself from the transaction response for the other participating members, and forwarding the remaining transaction response to the other participating members in reverse order of the path for sending the combined transaction request message to the service provider, until the first member receives its transaction response.

43. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a next member Xj,k (j=2,3,4.....; k=1,2,3.....m; m is a variable of type n; n=1,2,3...; m can be different values of j) if the second member is a message router;

combining a second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange request message to a next member Xj,k if the second member is a participating member;

sending the combined key exchange request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to the next member Xj,k, if the current member Xj,k, is a participating member;

sending the combined key exchange request to a service provider if the current member is the last participating member;

generating at the service provider different session keys for different participating members;

formatting, by the service provider, into one message, a key exchange response message including the different session keys for different participating member and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating, the key exchange response message for itself from the key exchange response messages for the other participating members in reverse order of the path for sending the key exchange request to the service provider, until the first member receives its key exchange response message.

44. The method of claim 13 or 14 of conducting a transaction using session keys between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:

formatting a transaction request message at a first member;

sending the transaction request message from the first member to a next member Xj,k (j = 2, 3, 4, . . . ; k = 1, 2, 3, . . . m; m is a variable of type n; n= 1, 2, 3, . . . ; m can be different values of j) if the second member is a message router;

combining a second member's transaction request message with the first member's transaction request message and sending the combined transaction request message to a next member Xj,k if the second member is a participating member;

sending the combined transaction request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's transaction request message with a previous member's transaction request message and sending the combined transaction request message to the next party Xj,k if the current member Xj,k a participating member;

sending the combined transaction request to a service provider if the current member is the last participating member or message router;

formatting, by the service provider, into one message, a transaction response message for each participating member and sending the combined transaction response message in reverse order of the path for each participating member and sending the combined transaction request to the service provider; and

separating, by every participating, transaction response message for itself from the transaction response messages for the other participating members in reverse order of the path for sending the transaction request to the service provider, until the first member receives its transaction response message.

45. The method of claim 13 or 14 of conducting a key exchange between two members and a service provider comprises the steps of:

sending a key exchange request message from the first member to a second member;

combining at the second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating at the service provider a session key used for both the first member and the second member;

formatting a key exchange response message at the service provider including the session key for the first member, signing the response message, formatting a key exchange response message including the session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

46. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in series comprising the steps of:

formatting a key exchange request message at a first member;

sending the key exchange request message from the first member to a second member

~~where the second member is a message router or participating member;~~

~~sending a key exchange request message from the second member to a next member, if the second member is a message router;~~

~~combining the second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange message to the next member if the second member is a participating member;~~

~~sending the combined key exchange request message to the next member if the current member is a message router;~~

~~combining a current member's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to a next member, if the current member is a participating member;~~

~~sending the combined key exchange request to a service provider if the current member is the last participating member or message router;~~

~~generating at the service provider a session key for the participating members;~~

~~formatting, by the service provider, into one message, a key exchange response message including the session key for the participating members and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and~~

~~separating, by every participating member, the key exchange response message for itself from the key exchange response messages for the other participating members, and forwarding the remaining key exchange response messages to the other participating members in reverse order of the path for sending the combined key exchange request to the service provider, until the first member receives its key exchange response message.~~

~~47. The method of claim 13 or 14 of conducting a key exchange between multiple members and a service provider arranged in a hierarchical organization comprising the steps of:~~

~~formatting a key exchange request message at a first member;~~

~~sending the key exchange request message from the first member to a next member Xj,k (j=2,3,4.....; k=1,2,3.....m; m is a variable of type n; n=1,2,3...; m can be different values of j) if the second member is a message router;~~

combining a second member's key exchange request message with the first member's key exchange request message and sending the combined key exchange request message to a next member Xj,k if the second member is a participating member;

sending the combined key exchange request message to the next member Xj,k if a current member Xj,k is a message router;

combining a current member Xj,k's key exchange request message with a previous member's key exchange request message and sending the combined key exchange request message to the next member Xj,k, if the current member Xj,k, is a participating member; sending the combined key exchange request to a service provider if the current member is the last participating member or message router;

generating at the service provider a session key for the participating members;

formatting, by the service provider, into one message, a key exchange response message including the session key for the participating member and sending the combined key exchange response message in reverse order of the path for sending the combined key exchange request to the service provider; and

separating, by every participating, the key exchange response message for itself from the key exchange response messages for the other participating members in reverse order of the path for sending the key exchange request to the service provider, until the first member receives its key exchange response message.

48. The method of claim 38 wherein the service provider provides each member involved in a transaction with other member's public keys.

49. The method of claim 41 wherein the service provider provides each member involved in a transaction with other member's public keys.

50. The method of claim 43 wherein the service provider provides each member involved in a transaction with other member's public keys.

51. The method of claim 45 wherein the service provider provides each member

~~involved in a transaction with other member's public keys.~~

a

~~52. The method of claim 46 wherein the service provider provides each member involved in a transaction with other member's public keys.~~

~~53. The method of claim 47 wherein the service provider provides each member involved in a transaction with other member's public keys.~~

add a2